IN THE CLAIMS

Please amend the claims as follows:

1-23. (canceled)

24. (currently amended) A method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network;

a) storing the computed first hash values;

b) computing current hash values for the replicas of the resource;

c) comparing the current and first hash values in order to identify whether all the hash values match, wherein nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first has value;

d) detecting that ~~whether~~ a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of ~~at least one~~ changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one; and ~~wherein the detecting comprises:~~

~~detecting whether the at least one changed replica is greater in number than a predetermined number; and~~

~~wherein the method further comprises:~~

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded.

25. (previously presented) The method of claim 24, wherein steps a), b), c), and d) are performed at a first data processing system within the network.

26. (previously presented) The method of claim 24, wherein step b) is performed at each replica's respective data processing system, the method further comprising sending the computed hash values to a first data processing system.

27. (previously presented) The method of claim 24, wherein the vulnerability includes a vulnerability to a computer virus.

28. (previously presented) The method of claim 24, wherein the vulnerability includes a vulnerability to computer hacking.

29. (previously presented) The method of claim 24 further comprising:

classifying as vulnerable the data processing systems storing the replicas, wherein the classifying is responsive to the predetermined number of changed replicas of the resource being exceeded.

30. (previously presented) The method of claim 24, the steps further comprising:

sending a notification of the vulnerability to each data processing system storing one of the replicas;

selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability; and

sending the selected instructions to each of the data processing systems storing one of the replicas.

31. (currently amended) An apparatus comprising:

a processor; and

a storage device connected to the processor, wherein the storage device has stored thereon a program, wherein the processor is operative to execute instructions of the program to implement a method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network;

a) storing the computed first hash values;

b) computing current hash values for the replicas of the resource;

c) comparing the current and first hash values in order to identify whether all the hash values match, wherein nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first has value;

d) detecting that ~~whether~~ a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of ~~at least one~~ changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one; and ~~wherein the detecting comprises:~~

~~detecting whether the at least one changed replica is greater in number than a predetermined number; and~~

~~wherein the method further comprises:~~

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded.

32. (previously presented) The apparatus of claim 31, wherein steps a), b), c), and d) are performed at a first data processing system within the network.

33. (previously presented) The apparatus of claim 31, wherein step b) is performed at each replica's at respective data processing system, the method further comprising sending the computed hash values to a first data processing system.

34. (previously presented) The apparatus of claim 31, wherein the vulnerability includes a vulnerability to a computer virus.

35. (previously presented) The apparatus of claim 31, wherein the vulnerability includes a vulnerability to computer hacking.

36. (previously presented) The apparatus of claim 31, the steps further comprising:

classifying as vulnerable the data processing systems storing the replicas, wherein the classifying is responsive to the predetermined number of changed replicas of the resource being exceeded.

37. (previously presented) The apparatus of claim 31, the steps further comprising:

sending a notification of the vulnerability to each data processing system storing one of the replicas;

selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability; and

sending the selected instructions to each of the data processing systems storing one of the replicas.

38. (currently amended) A computer program product, stored on a tangible, computer readable medium, said computer program product having instructions for execution by a computer system, wherein the instructions, when executed by the computer system, cause the computer system to implement a method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network;

a) storing the computed first hash values;

b) computing current hash values for the replicas of the resource;

c) comparing the current and first hash values in order to identify whether all the hash values match, wherein nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first has value;

d) detecting that ~~whether~~ a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of ~~at least one~~ changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas, wherein the predetermined number is at least one; and ~~wherein the detecting comprises:~~

~~detecting whether the at least one changed replica is greater in number than a predetermined number; and~~

~~wherein the method further comprises:~~

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded.

39. (previously presented) The computer program product of claim 38, wherein steps a), b), c), and d) are performed at a first data processing system within the network.

40. (previously presented) The computer program product of claim 38, wherein step b) is performed at each replica's respective data processing system, the method further comprising sending the computed hash values to a first data processing system.

41. (previously presented) The computer program product of claim 38, wherein the vulnerability includes a vulnerability to a computer virus.

42. (previously presented) The computer program product of claim 38, wherein the vulnerability includes a vulnerability to computer hacking.

43. (previously presented) The computer program product of claim 38, the steps further comprising:

classifying as vulnerable the data processing systems storing the replicas, wherein the classifying is responsive to the predetermined number of changed replicas of the resource being exceeded.

44. (previously presented) The computer program product of claim 38, the steps further comprising:

sending a notification of the vulnerability to each data processing system storing one of the replicas;

selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability; and

sending the selected instructions to each of the data processing systems storing one of the replicas.